Sub A1

CLAIMS

What is claimed is:

1. A cryptographic method comprising the steps of:

receiving physical characteristic information representing a characteristic inherent to an individual;

randomly determining a numeric key;

generating a cryptographic key from said numeric key and a predetermined primary key;

encrypting said physical characteristic information using said cryptographic key; and

generating an auxiliary code for decrypting said cryptographic key ,from said encrypted physical characteristic information and said numeric key.

2. A decryption method comprising the steps of:

receiving encrypted physical characteristic information and an auxiliary code;

restoring a numeric key from said received data;

restoring cryptographic key from said numeric key and a predetermined primary key; and

decrypting said encrypted physical characteristic information by using said cryptographic key and obtaining physical characteristic information.

3. A cryptographic equipment, comprising:

inputting means for inputting physical characteristic information representing a characteristic inherent to an individual;

numeric key generating means for randomly determining numeric key;

key generating means for generating a cryptographic key from said numeric key and a predetermined primary key;

encrypting means for encrypting said physical characteristic information using said cryptographic key; and

code generating means for generating an auxiliary code from said encrypted physical characteristic information and said numeric key.

4. A decryption equipment comprising:

receiving means for receiving an encrypted physical

characteristic information and an auxiliary code ;

numeric key restoring means for restoring a numeric key from said encrypted physical characteristic information and said auxiliary code;

key generating means for generating a cryptographic key from said numeric key and a predetermined primary key; and

decrypting means for decrypting said encrypted physical characteristic information by using said cryptographic key.

5. A storage media for storing a program to be executed by a computer, comprising:

a inputting procedure for inputting physical characteristic information representing a characteristic inherent to an individual;

a numeric key generating procedure for randomly determining a numeric key;

a key generating procedure for generating a cryptographic key from said numeric key and a predetermined primary key;

an encrypting procedure for encrypting said physical characteristic information using said cryptographic key; and

a code generating procedure for generating an auxiliary code from said encrypted physical characteristic information and said numeric key.

6. A storage media for storing a program to be executed by a computer, comprising:

a receiving procedure for receiving a cryptogram including an encrypted physical characteristic information and an auxiliary code;

a numeric key restoring procedure for restoring a numeric key from said encrypted physical characteristic information and said auxiliary code;

a key generating procedure for generating a cryptographic key from said numeric key and a predetermined primary key; and

a decrypting procedure for decrypting said encrypted physical characteristic information by using said cryptographic key.

7. An cryptographic method comprising the steps of:

receiving physical characteristic information

representing a characteristic inherent to an individual;

arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information; and

encrypting the scrambled physical characteristic information by using the predetermined cryptographic key.

8. A decryption method comprising the steps of:

receiving a cryptogram which is an encryption of scrambled physical characteristic information;

decrypting said cryptogram by using the predetermined cryptographic key and obtaining said scrambled physical characteristic information ; and

descrambling said scrambled physical characteristic information by removing each element from each component constructing the result of decryption, in which each element is effected at the time of scrambling, by a plurality of components that has a predetermined relationship with said each component.

9. A cryptographic equipment comprising:

inputting means for inputting physical characteristic information representing a characteristic inherent to an individual;

scrambling means for arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information; and

encrypting means for encrypting the scrambled physical characteristic information by using the predetermined cryptographic key.

10. A decryption equipment comprising decrypting means for decrypting a received cryptogram which is an encryption of a scrambled physical characteristic information, by a

predetermined cryptographic key and obtaining said scrambled physical characteristic information and

descrambling means for descrambling said scrambled physical characteristic information.

11. A storage media for storing a program to be executed by a computer, comprising:

a inputting procedure for inputting physical characteristic information representing a characteristic inherent to an individual;

a scrambling procedure for arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information; and

an encrypting procedure for encrypting the scrambled physical characteristic information by using the predetermined cryptographic key.

12. A storage media for storing a program to be executed by a computer, comprising a decrypting procedure for decrypting a received cryptogram which is an encryption of a scrambled physical characteristic information, by a predetermined cryptographic key and obtaining said scrambled physical characteristic information and

a descrambling procedure for descrambling said scrambled physical characteristic information.

13. A remote identification system comprises a client-side equipment and server-side equipment , wherein:

said client-side equipment comprising inputting means for inputting physical characteristic information representing a characteristic inherent to an individual;

proof information inputting means for inputting information including identifier or identifying an individual and a password;

encrypting means for encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram; and

outputting means for outputting authenticating information generated from said cryptogram and said identifier;

said server-side equipment comprising registering means for registering password and reference data which is obtained by measuring a physical characteristic corresponding to each individual, relating to given identifier corresponding to each person;

receiving means for receiving authenticating information consisting of said cryptogram and said identifier;

retrieving means for retrieving a relating password and reference data from said registering means in accordance to received identifier ;

decrypting means for decrypting said received cryptogram by using the password retrieved by said retrieving means as a cryptographic key and obtaining a physical characteristic information; and

examining means for examining whether or not said physical characteristic information and retrieved reference data are equivalent.

14. A data sending equipment comprising:

inputting means for inputting physical characteristic information representing a characteristic inherent to each individual;

proof information inputting means for inputting information including identifier or identifying an individual and a password;

encrypting means for encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram; and

outputting means for outputting authenticating information generated from said cryptogram and said identifier.

15. A identifying equipment comprising:

registering means for registering password and reference data which is obtained by measuring a physical characteristic corresponding to each individual, relating to given identifier

corresponding to each person;

receiving means for receiving authenticating information consisting of said cryptogram and said identifier;

retrieving means for retrieving a relating password and reference data from said registering means in accordance to received identifier ;

decrypting means for decrypting said received cryptogram by using the password retrieved by said retrieving means as a cryptographic key and obtaining a physical characteristic information; and

examining means for examining whether or not said physical characteristic information and retrieved reference data are equivalent.